EU/G7 Healthcards - WG7

Interoperability of Healthcard Systems
Part 1

General Concepts

Prepared by

Dr David Markwell, MB BS.

(as coordinator of EU/G7 Healthcards WG7 Interoperability)

ADDRESS FOR COMMENTS

The Clinical Information Consultancy,
93 Wantage Road, Reading, Berkshire, RG30 2SN, UK
Tel +44-1734 584954   Fax +44-1734 504464
Email dmarkwell@cix.compulink.co.uk

Web site: http://www.compulink.co.uk/~cic/euhci.htm

THIS DOCUMENT IS FOR DISCUSSION AS THE BASIS FOR A CONSENSUS BETWEEN EU HEALTHCARD PROJECTS

IT MAY BE SUBJECT TO FINAL REVISION FOLLOWING THE CONSENSUS MEETING ON 3 JULY 1996

Comments on any major substantive issues requiring discussion at the consensus meeting MUST be received by 30 June 1996 comments must be sent by post, fax or e-mail to David Markwell at the above address

Table of contents

Interoperability of Healthcard Systems

Final version - Part 1 - General Concepts

1 Preface

This document is the first of three parts of the Working Document of the Healthcard Interoperability Feasibility Study. It introduces general concepts related to healthcare interoperability and provides a framework for the more detailed considerations in Part 2 and for the interoperability specification in Part 3.

This document is based on earlier work in the EU concerted action Eurocards, revised to take account of discussions in the EU healthcard Feasibility Study - Core Technical Group (CTG) during the first half of 1996. It is to be discussed as the basis for agreement between EU funded healthcard projects at a consensus meeting on 3 July 1996. Subject to the outcome of that meeting, a Final Report incorporating last minute revisions will be available by 15 July 1996.

The parts of the document are available in Microsoft Word™ 6.0 files. These files are named in accordance with the following convention – – EUHCI*[a]-[n]*.DOC

> *[a]* is a letter signifying the version of the document.

> *[n]* is a digit signifying the part of the document.

Revisions since previous draft (1.0)

1. Changes to headers and front page only to align with Parts 2 and 3. No changes to text.

Advice to readers

If you are familiar with previous work in Eurocards or with earlier drafts of this document you may prefer to skip directly to Part 2 or 3 of the report.

---

2 Introduction

Interoperability between Healthcard Systems is the ability of one Healthcard System to read, use and/or update the data, on Healthcards issued by another Healthcard System.

A Healthcard System is the sum of the Healthcards issued and all the hardware and software used in a particular implementation.

The considerations about interoperability in this section apply, at one extreme, to two identical systems and, at the other extreme, to two completely different systems one or both of which have been extended in some way to allow access to Healthcards issued by the other.

Various possible levels of interoperability are illustrated by considering the ability of one Healthcard System to read and/or write cards issued by another Healthcard System. Interoperability may be symmetrical (i.e. both Healthcard Systems have similar capabilities for accessing each other's cards) or asymmetrical (i.e. one Healthcard System can access the cards issued by the other Healthcard System but this facility is not reciprocated). The situation becomes more complex with three or more systems since the extent of interoperability between different pairs of system may vary.

The issue of healthcard interoperability can be divided into three distinct areas.

- Functional interoperability of healthcard systems
    - Some or all of the functions of one Healthcard System make use of and/or update computer readable data held on the Healthcards issued by another Healthcard System.

- Technical interoperability of healthcard systems
    - Some or all of the computer readable data on cards issued by one Healthcard System can be read by one or more Card Access System (CAS) in another Healthcard System.

- Technical interoperability of healthcard system components
    - One or more of the components of one Healthcard System can be interchanged with the equivalent component of another Healthcard System without impeding or changing the overall operation of the Healthcard System.

3 Functional interoperability between Healthcard Systems

True functional interoperability occurs when some or all of the functions of one Healthcard System make use of or update computer readable data held on the Healthcards issued by another Healthcard System.

3.1 Advantages of functional interoperability

3.1.1 Healthcare

- Administrative:
    – Simplification of administrative procedures for the patient (e.g. E111 function);
    – Identification of the healthcare professional usually responsible for care of the patient to allow information to be requested to assist in treatment;
    – Use of the Healthcard to authorise access to patient records by network.

- Clinical:
    – Access to accurate emergency and other clinical information held on the Healthcard when and where it is needed (rather than just in the issuing system);
    – Reduction of delays to treatment of patients due delays in accessing relevant clinical information about the patient.

3.1.2 Health economics

- More efficient administrative procedures when treating a patient covered by another Healthcard System;
- Simplification of billing or claiming for services provided to a patient participating in another Healthcard System;
- A standard Healthcard System specification would reduce the cost of development, implementation, support and training;
- An interoperable Healthcard System may form a basis for improved interworking between other patient-centred information systems;
- Similar Healthcard System systems will facilitate the mobility of staff between different hospitals or organisations.

3.1.3 Political

- Interoperable Healthcard Systems crossing national boundaries would be a practical demonstration of cooperation within the European Union and in other G7 countries;
- Benefits to healthcare services and industrial partners in all Member States through creation of a more stable market for Healthcard System products.

3.1.4 Commercial

- Increased sales of Healthcards, Card Terminals and Healthcard System services based on a common specification;
- Simpler maintenance of healthcare applications that only have to support a single Healthcard interface.

3.2 Obstacles to functional interoperability

3.2.1 Healthcare

- Differences in views about the requirements that may be met with Healthcards;

- Lack of data protection harmonisation in relation to healthcare data.

3.2.2 Health economics

- Current investments in incompatible information systems;

- Current investments in incompatible Healthcard trials and implementations;

- Lack of appropriate infrastructure;

- Competition between insurers and providers.

3.2.3 Political

- Competition between Member States seeking to benefit their own healthcare system or industry.

3.2.4 Commercial

- Competition between suppliers of cards using different media;

- Competition between suppliers of cards using similar media with proprietary interfaces;

- Commercial/academic competition between those involved in different approaches and trials.

3.2.5 Technological

- Lack of agreement on the optimum technology for Healthcards;

- Continuing development of alternative technologies.

3.3 Prerequisites for functional interoperability

There are three prerequisites for functional interoperability

- Technical interoperability of Healthcard Systems

  – See section 5.

- Common functions and/or data requirements

  – Functionally interoperable Healthcard Systems must either share some common functions or, at least, functions that utilise common data sets. Functional interoperability is inevitably limited to these areas of common functionality even if the cards and Card Terminals are technically identical.

  – Any discussion of interoperability must identify the functions that are to be made interoperable and the data required to support those functions.

  – Consideration should be given to which components of each Healthcard System support the interoperable functions.

    – A card and its interface may support the reading and writing of a set of data required to support a particular function. However, functional interoperability is not possible unless the applications support access to this data.

  – Consideration should also be given to the patterns of use applied by users of the Healthcard System.

    – A card, its interface and the application may support the reading and writing of a set of data required to support a particular function. However, if for any reason one the users do not record the necessary data on the card the apparent interoperability will not be realised.

- An interoperability agreement

  – See section 4.

4 Interoperability agreements

4.1 The need for interoperability agreements

Interoperability complicates data management because it increases the number of organisations that may have access to the data. The objective of interoperability should not be allowed to obscure the potential threat to confidentiality.

Interoperability effects confidentiality of data written to the Healthcard by either system. If one system restricts access to particular data-items to certain categories of user, the question arises as to whether this restriction is enforced by other interoperable systems and if so how.

If a Healthcard System can update data on cards issued by another Healthcard System this complicates the issue of responsibility for the accuracy of Healthcard information.

Interoperability agreements[1] must be established between any Healthcard Systems that are functionally interoperable. These agreements must clearly specify the extent of any right to read and/or update data on a PCD issued by the other Healthcard System. The agreements should specify technical safeguards and management procedures to ensure that the agreement is implemented effectively. The agreements must also establish mechanisms for dealing with problems arising from interworking, in particular for resolving disputes about responsibilities for errors.

4.2 Interoperability and data protection

If interoperable Healthcard Systems cross national boundaries, the interoperability agreements must be compatible with data protection legislation in each country in which the Healthcards concerned may be used.

4.3 Interoperability and acceptance of data

There is no point in making systems interoperable if the users are unable or unwilling to accept data entered by users of the other Healthcard System. For example, if a provider cannot use Healthcard data for E111 eligibility there is little point in them being able to read this data. Similarly, if an insurer involved in one Healthcard System is unwilling to accept the validity of a claim issued by a hospital involved in the other Healthcard System, even if it is validated by a Healthcard issued by their own Healthcard System, interoperability of this function is pointless.

4.4 Interoperability with Central Reference Databases

Either or both of a pair of interoperable Healthcard Systems may include a Central Reference Database (CRD) for personalising and re-issuing cards (see Section 5.1.4). In this case, if the other Healthcard System can update Healthcard, arrangements must be made to capture these changes on the CRD. This may be difficult since a CAS involved in the other Healthcard System may not have any connection with the CRD.

---

[1] To some extent PCS interoperability agreements are analogous to the data interchange agreements between parties involved in Electronic Data Interchange (EDI). However, a PCS provides direct access to data held on a common media (Healthcard) and the recipient of the data contained on the Healthcard is not addressed specifically by the author of the data. Therefore PCS interoperability agreements should be more rigorous than EDI agreements.

5 Technical interoperability

5.1 Healthcard System Components

5.1.1 Overview

Figure 1 provides a diagrammatic representation of a Healthcard System consisting of the following components:

- Healthcards
    - A card containing computer-readable data that is issued to patients to facilitate the provision of healthcare.;
- Card Access Systems (CAS)
    - Systems that can read and/or write the computer-readable data.

5.1.2 Card Access System Components

- A Card Terminal
    - A device capable of communicating with a Healthcard.
- Additional hardware and/or software
    - To allow card data to be read and /or updated by a user. A user may be an organisation involved in the provision of healthcare, a healthcare professional or another person acting on behalf of or employed by a healthcare organisation or a patient.

5.1.3 Additional hardware and software associated with a CAS

There are many variations in the additional hardware or software that may be included in a particular CAS. The following descriptions and diagrams illustrate some of the many variants. A CAS may include:

- A screen or printer that displays or prints data from a Healthcard (see Figure 2).
- A keyboard or other input device used to select the data to be displayed and/or to update some or all of the Healthcard data (see Figure 3).
- A database holding copies of some or all of the Healthcard data (see Figure 4 and Figure 5).

One Healthcard System may include CASs with different ranges of functionality according to the requirements of the user.

5.1.4 Central Reference Databases

A Healthcard System may include a Central Reference Database (CRD) that may be used both to write the initial data to Healthcards and to hold a backup copy of the Healthcard data. If CASs are able to update Healthcard data that is also stored by the CRD, they require a means of electronic communication with the CRD to keep the data on the CRD consistent with the Healthcard data. CASs that are not able to update the data stored on the Healthcard data derived from the CRD need not communicate with the CRD.
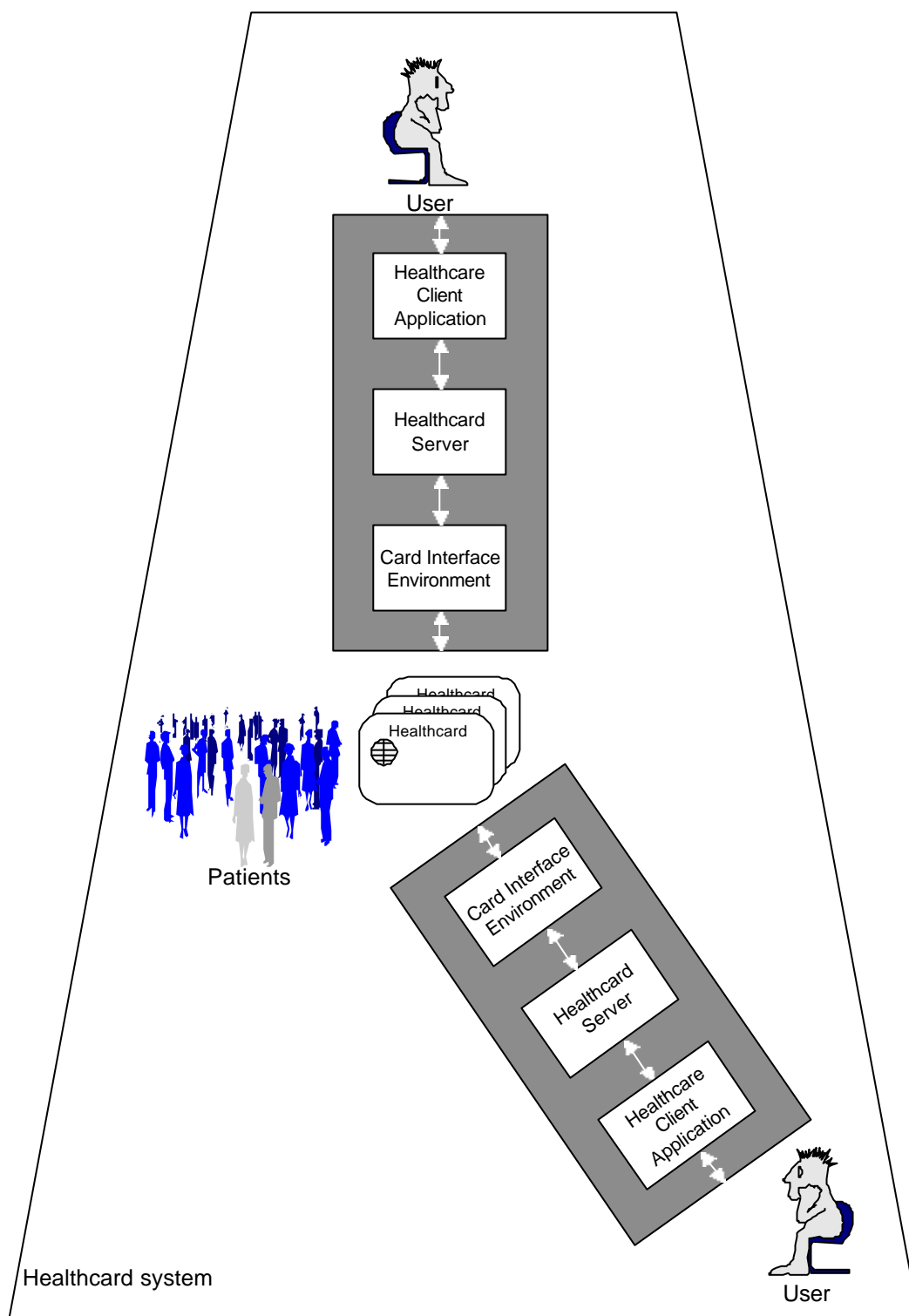
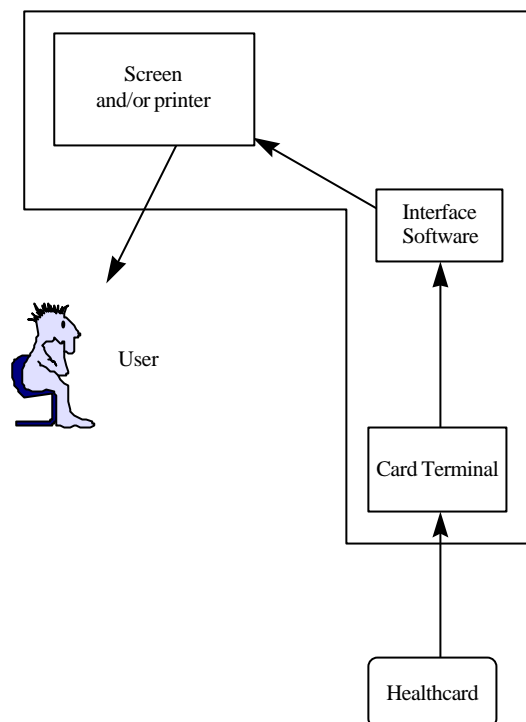**Figure 1. The components of a Healthcard System**

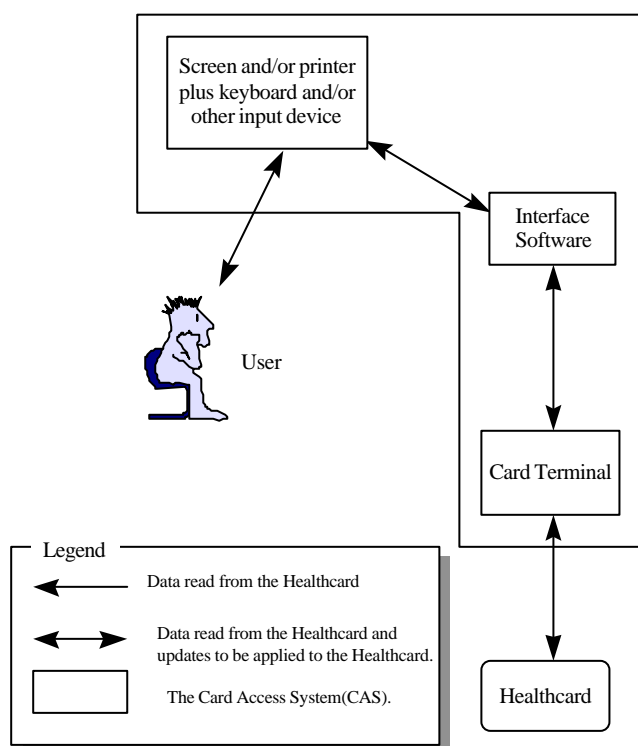**Figure 2. A simple read-only Card Access System**

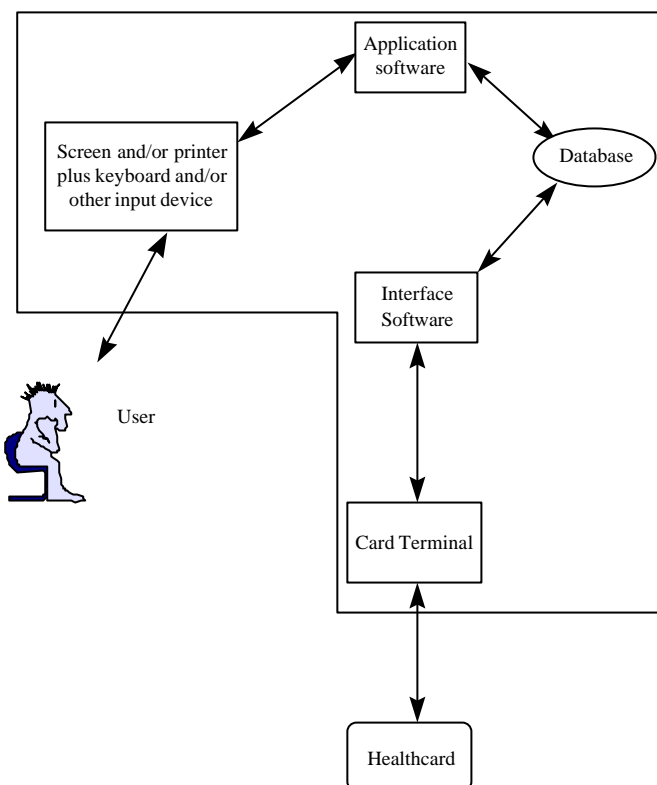**Figure 3. A simple Card Access System that supports healthcard updates**

Figure 4. The Card Access System integrated with a database
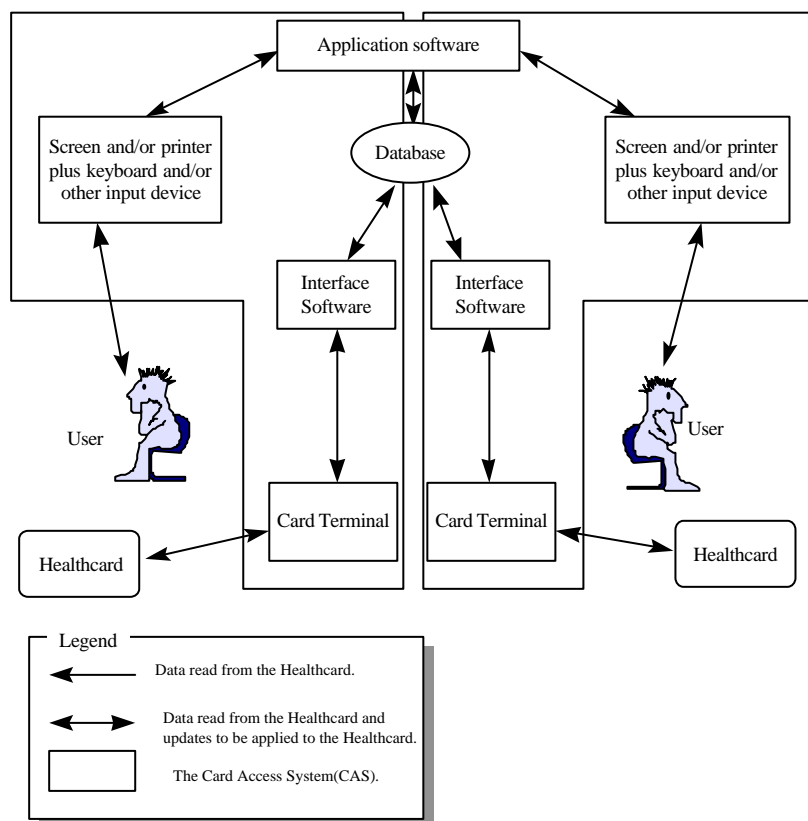
Figure 5. A multi-user Card Access System integrated with a database

5.2 Card access

To understand the various components that determine the technical interoperability of Healthcard Systems it is necessary to understand the way in which a Healthcard may be accessed by the user of a Healthcard System.

Figure 6 illustrates the components of a CAS and the data flows from (white arrows) and to (grey arrows) a Healthcard. It shows a super-set of the components and data-flows associated with access to a Healthcard. Different Healthcard Systems may include different combinations of these components and data-flows. Interoperability may be limited by the nature and content of the data-flows supported by different Healthcard Systems. The components and data-flows identified in the diagram are summarised in Table 1 and Table 2.
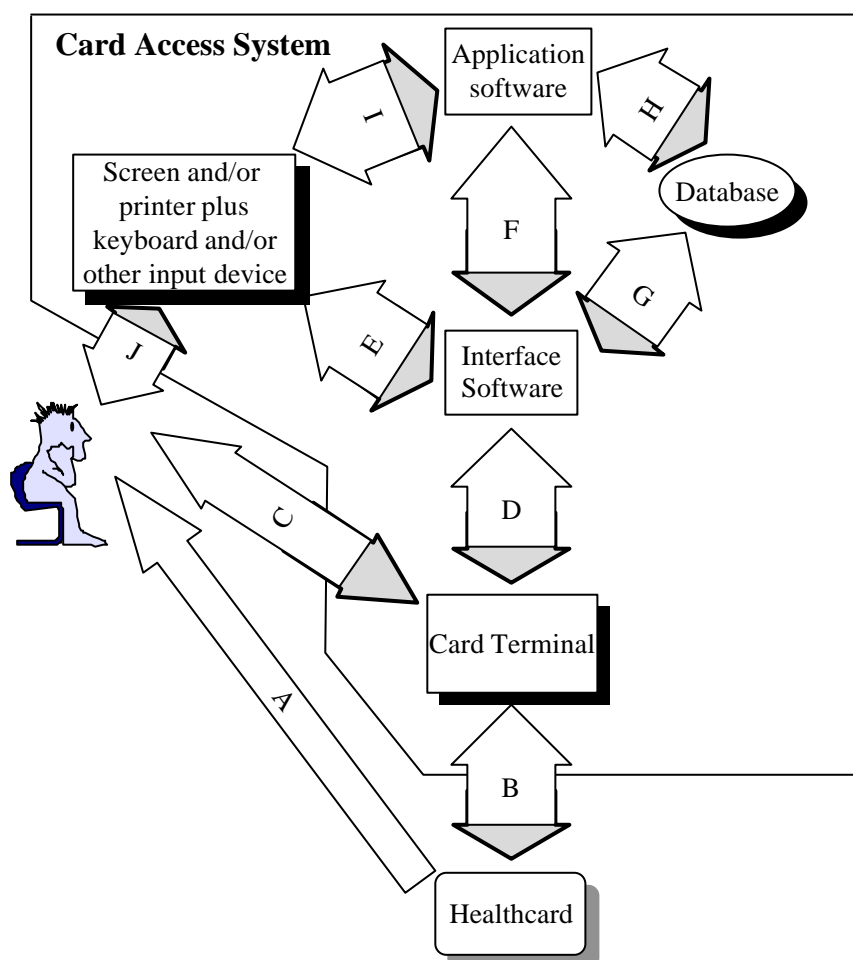
Refer to Table 1 for description of components.

Refer to Table 2 for key to data flows.

There may be an additional set of data flows to and from an external Central Reference Database. These are not shown in this diagram.

Figure 6. Card Access System components and data-flows

Table 1. Card Access System components

Component	Description	Notes
Healthcard	The Healthcard	The Healthcard will contain a limited amount of visible data and a variable amount of computer-readable data.
		The computer-readable data may be stored in one or more types of media on or inside the Healthcard. There are three general types of computer-readable media (i.e. magnetic, optical and integrated circuit). However, there are several variations of each of these general types[2].
		Some integrated circuit cards may process instructions from the Card Terminal, while the role of other media is passive.
Card Terminal	A device that connects to or communicates directly with a Healthcard to read data from it or to update it with new or changed data.	A Card Terminal may be a device that connects electrically to the Healthcard (as for an integrated circuit card) or a device that reads the medium by scanning or swiping magnetically or optically recorded data.
		The Card Terminal may be a passive link between the Healthcard and interface-software. However, some Card Terminals are able to process instructions, read or write data selectively and interact with a processor within the Healthcard.
		More sophisticated Card Terminals may incorporate a key pad and/or a screen for data viewing.

---

[2] A full description of the different technologies that can be used to provide computer-readable media on a Healthcard is beyond the scope of this report. EUROCARDS Working Group 2 studied and reported on this aspect of Healthcards. In the context of this chapter the significant point is that different card media require different reader writer components in the card terminal.

Component	Description	Notes
Interface-software	Software that is specifically required to allow access to data on a Healthcard.	The interface-software processes data read from a Healthcard and the data that is to be written to a Healthcard. The interface-software may present data read from a Healthcard on a screen or in a printed report. Alternatively the data may be used to update an application database. The interface-software may update the Healthcard with data that has been specifically entered for this purpose or with data derived from an application database. The interface-software may need to issue instructions to the Card Terminal to initiate card reading or updating.
Database	A database accessed by the application software.	The database may hold: A copy of the data held on the Healthcard; Other data about the patient that are accessible with or without the Healthcard; Data about the health professional or organisation that may be combined with Healthcard data to generate forms or electronic transactions or additional data to be added tot the Healthcard.
Application software	Software that is not specific to Healthcard access but which is integrated with the Healthcard System.	Application software may be used to read the application database and thus to indirectly ascertain the contents of a Healthcard. Similarly it may allow the database to be updated by the user and these updates may be written to the card. If a Healthcard may be accessed by different types of healthcare professional and by different healthcare organisations several different applications with different databases must be able to interface with the same type of Healthcard.

Table 2. Healthcard access data-flows

Flow	Description	Data-flow from the Healthcard	Data-flow to the Healthcard
A	User reads visible data from the Healthcard.	Visible data.	None.
B	Connection of Healthcard to Card Terminal. The nature of the connection depends on the computer-readable storage media on the Healthcard.	Data.	Data. Security keys. Instructions: If the Healthcard medium has processing capacity (e.g. smart cards)
C	Direct input or output from a Card Terminal including a keypad and screen.	Prompts for input: See next column. Data: Limited by viewing facility of Card Terminal.	PIN codes or other security keys: Entered directly on a Card Terminal keypad.
D	Connection of Card Terminal to computer. A serial or parallel link (e.g. RS232, Centronics, SCSI etc.).	Data. Status information.	Data. Instructions. PIN codes or other security keys.

Flow	Description	Data-flow from the Healthcard	Data-flow to the Healthcard

E	"Direct" viewing and updating of Healthcard data.	Data:
		
		    In a human-readable form.
		
		Prompts for input.
			Data:
			
			    As entered by the user.
			
			PIN codes or other security data.
			
			Instructions.

F	Communication between the card and application software.	Identifiers or keys:
		
		    Used to identify records or unlock security features in the application software.
		
		Data:
		
		    To be merged with data from the application database before displaying or printing.
			Instructions:
			
			    From the application software to initiate reading or updating of the Healthcard.

G	Reconciliation of the application database and the Healthcard data.	Data:
		
		    To update the application database.
			Data:
			
			    From the application database.

H	Database access	Data:
		
		    From the application database for use by application software functions or to display or print.
			Data:
			
			    To update the application. database.

I	Application interface	Data: From the application database and Healthcard. Prompts for input.	Data. Instructions. PIN codes or other security keys.
J	User interface	Screen views. Printed reports. Completed paper forms.	Keyboard or other input of data or instructions.

5.3 Levels of technical interoperability

Two systems in which the components and data-flows illustrated in Figure 6, Table 1 and Table 2 are identical in every respect are technically completely interoperable. This situation is unlikely unless all the components of both Healthcard Systems originate from the same suppliers. However, complete technical interoperability can also be achieved without absolute uniformity. Furthermore, there are many lesser degrees of interoperability that may meet specific requirements for specific functions.

In the following sections various possible levels of technical interoperability are considered. Each of these is illustrated by a diagram showing the data-flows and functions supported by Healthcards at different Card Access Systems (CASs). These represent only a few of the possible variants of technical interoperability between two systems. In practical implementations, combinations of these different generalisations of interoperability may apply between different CASs in each Healthcard System.

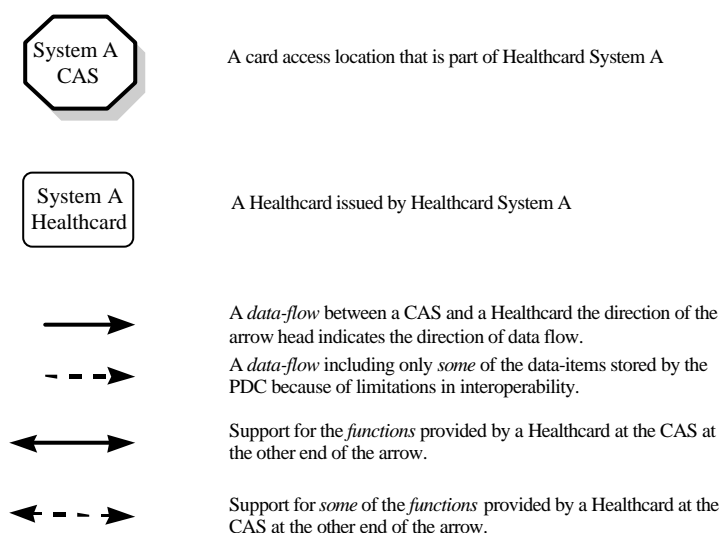The notation used in these diagrams is explained in Figure 7.

Figure 7. The notation used to illustrate different levels of interoperability

5.3.1 Complete technical interoperability

The following are the minimum requirements for complete interoperability between two systems:

a) The visible data must have the same content on Healthcards issued by both Healthcard Systems and the layout of the visible data must (if different) be recognisable by users of the other Healthcard System so that data-flow A is possible.

b) The Healthcards and Card Terminals used by the two Healthcard Systems must either be the same or must be interchangeable with one another in a way that allows data-flow B to be fully supported between the Card Terminals used by one system and the Healthcards used by the other system.

c) The application software and user interface must allow the user to read all the Healthcard data relevant to them (i.e. the flow of data towards the user, indicated by J, must meet the users requirements).

d) The application software and user interface must allow the user to update any of the Healthcard data that is relevant to them (i.e. the flow of data from the user, indicated by J, must meet the users requirements).

e) The interface-software must be designed to map between the application database and/or user interface and the shared data-flow D.

f) If either system requires a PIN or other key to be entered directly to the Card Terminal (data-flow C) rather than via the interface-software (data-flow D) then both systems must support this.

Complete interoperability of a Healthcard System can be achieved without dictating the processing or storage of the data by the information system used at a card access location. (CAS).
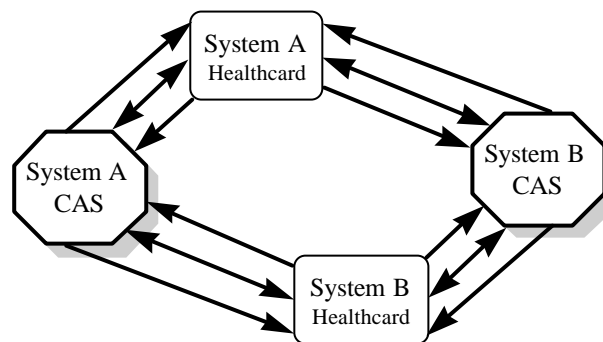

Figure 8. Complete interoperability

5.3.2 Interoperability with a limited range of functions

Two Healthcard Systems may be interoperable only for a limited range of functions provided by the individual Healthcard Systems. For example, a Healthcard may be interoperable between two systems for the purposes of identifying the patient or establishing their E111 entitlement but not for unlocking access to medical records.
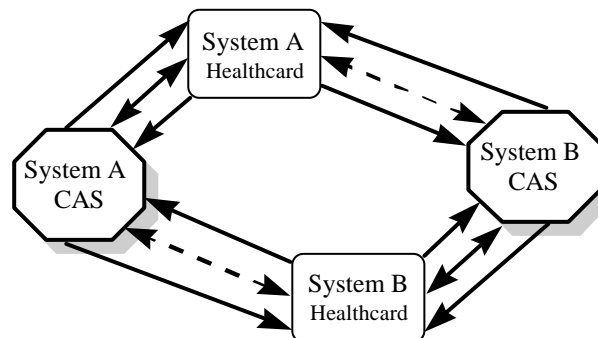

Figure 9. Functionally limited interoperability

5.3.3 Interoperability with limited data-sets

Similarly, interoperability may apply to a limited subset of the data stored on the Healthcards issued by these systems. For example, the name and date of birth of a patient stored on a Healthcard might be accessible by another Healthcard System but a statement of special insurance conditions might only be accessible by the issuing Healthcard System.
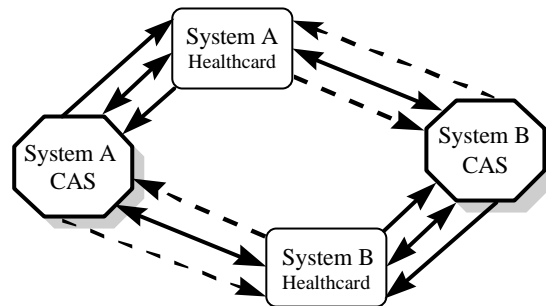

Figure 10. Data limited interoperability

5.3.4 Asymmetric interoperability

Interoperability between Healthcard Systems may be asymmetric. Healthcard System-A may be able to access data and functions of Healthcards issued by Healthcard System-B while Healthcard System-B is unable to access the same data and functions of Healthcards issued by Healthcard System-A. This situation may arise is two situations:

- If a new Healthcard System is designed that builds in support for Healthcards issued by an existing Healthcard System.

- If a Healthcard System is deliberately extended to accommodate Healthcards issued by another Healthcard System.
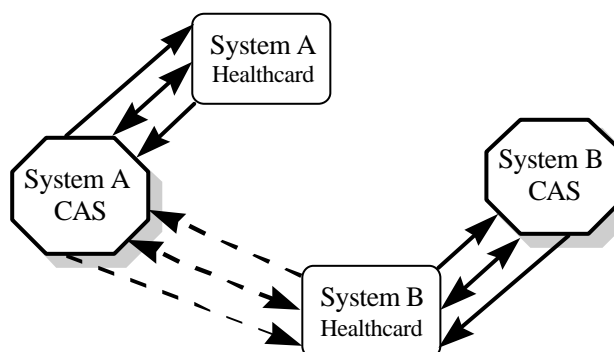

Figure 11. Asymmetric interoperability

Asymmetric interoperability need not be all-or-nothing. System B may have limited access to Healthcards issued by system A, while system A has a greater level of access to Healthcards issued by system B.

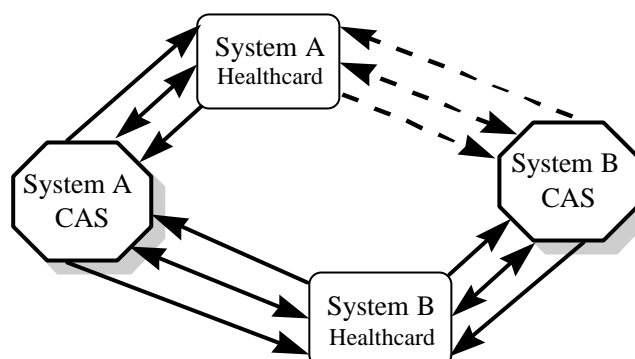**Figure 12. Asymmetric interoperability with limited symmetrical access**

5.3.5 Directionally limited interoperability

Interoperability between Healthcard System may be limited to the ability to read Healthcards issued by another Healthcard System. The ability to update the data held on a Healthcard may be restricted to the issuing Healthcard System.
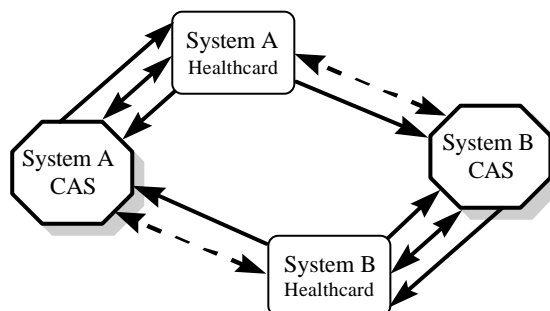
Figure 13. Directional interoperability

5.3.6 Location dependent interoperability

A Healthcard System may include card access locations which have different levels of interoperability with Healthcards issued by another Healthcard System.

An example of this might be that hospital systems in one country could read Healthcards issued by a Healthcard System in another country while interoperability might not be supported for pharmacy or dental systems. Another example might be that only CASs near to a geographical boundary between two Healthcard Systems were made interoperable.

Figure 14. Location dependent interoperability

5.4 Methods of achieving interoperability

In Section 5.1 the requirements for different levels of interoperability are outlined. In this section the methods by which some or all of these requirements may be met are considered.
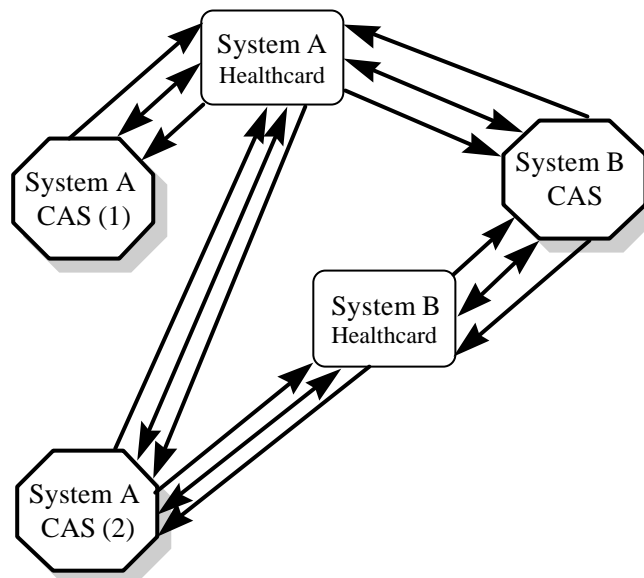
5.4.1 Dual systems

Two otherwise incompatible Healthcard Systems can be made interoperable by providing each user with two completely separate Card Access Systems (CASs). In this scenario each CAS consists of completely separate hardware and software designed to access Healthcards issued by one of the Healthcard Systems. The user recognises the type of Healthcard presented by the patient and uses the appropriate CAS.

This is obviously stretching the meaning of the term interoperable. However, in the absence of any more elegant solution, it is an approach which may be adopted if users need to access Healthcards issued by another scheme. The only advantage of this approach is that the Healthcard from the other scheme is managed by the hardware and software that it was designed to work with, reducing the risk of errors caused by differences between the systems.

There are many disadvantages:

- Cost of hardware and software;

- Difficulties for users having to work with different systems;

- Lack of integration of the Healthcard System with other operational systems.

While this may be a possible solution for a healthcare organisation on dealing with Healthcards issued by two overlapping Healthcard Systems it is impractical to extend the same approach to a third or fourth Healthcard System.

5.4.2 Parallel components

The system used to access a Healthcard can be subdivided into several hardware and software components (see Figure 6). Some of these components may be used to access Healthcards issued by other Healthcard Systems while others may need to be replaced by parallel components appropriate to the other Healthcard System. Figure 15 illustrates the duplication of components of a Healthcard access system to enable Healthcards issued by another Healthcard System to be read. It also illustrates how the processing of data from Healthcards issued by other systems may converge with and diverge from the processing of Healthcards issued by the Healthcard System that is normally used in that location. Figure 16 is a similar illustration of the process of updating Healthcards issued by other systems and Figure 17 shows the data-flows that some Healthcard Systems require to carry instructions to the interface, Card Terminal and/or Healthcard to initiate reading and updating of the card.

In Section 5.5 the possibilities for duplicating each of the main components of a Healthcard access system are considered and the likely impact of each of these is considered.
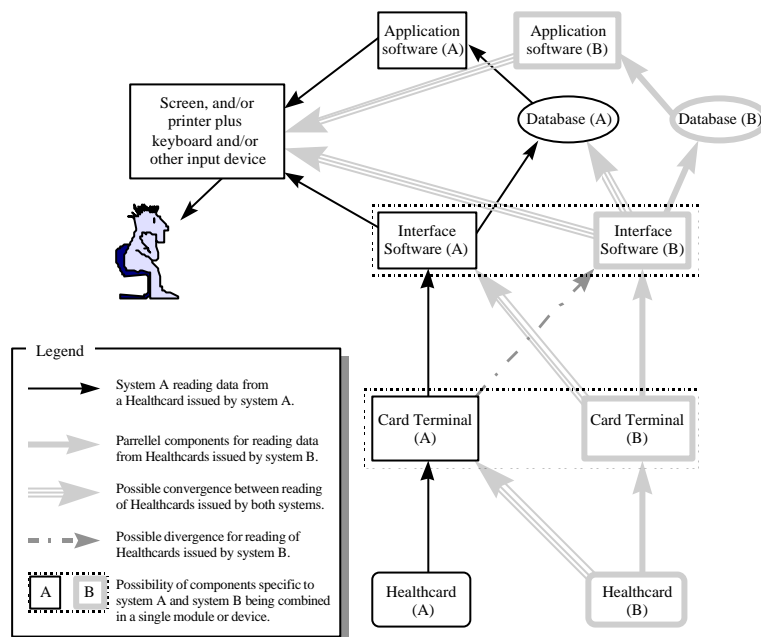
Figure 15. Possible ways of reading data from Healthcards issued by other systems
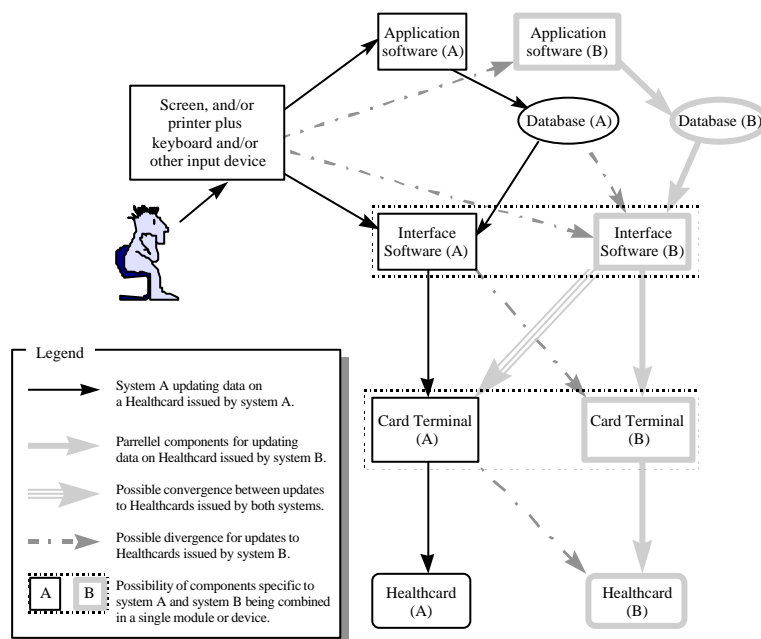
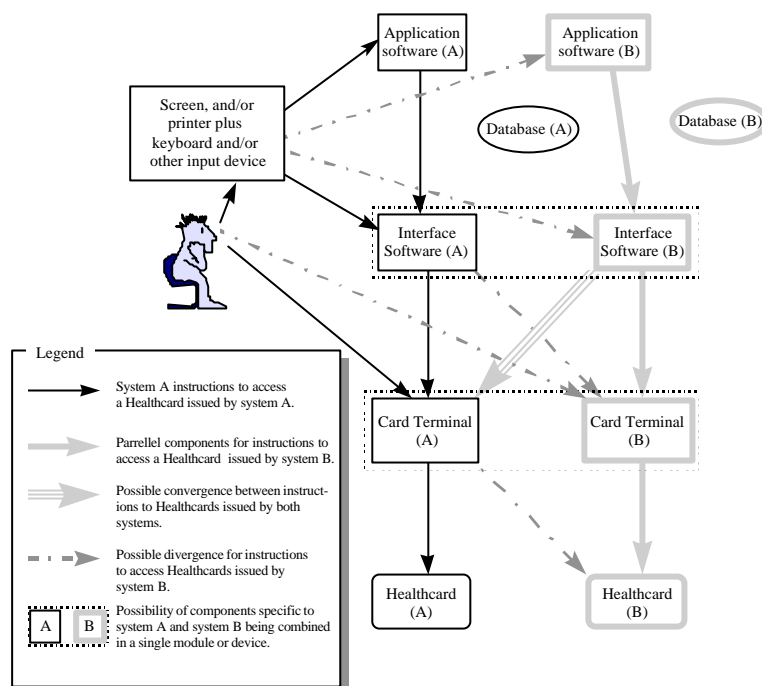**Figure 16. Possible ways of updating data on Healthcards issued by other systems**

Figure 17. Possible ways of sending instructions to Healthcards issued by other systems

5.5 Healthcard System components and interoperability

5.5.1 The card

Several properties of a Healthcard determine the extent to which it is accessible by a Healthcard System other than the one that issued it.

- The size of the Healthcard;

- The physical media in which the data is stored:

  - Magnetic stripe, integrated circuit, optical, etc

- The physical format of the data stored on the media:

  - For magnetic/optical media the density, method of recording, etc.

  - For integrated circuit cards contact positions, voltages, memory addressing, security features, etc.

- The logical structure of the data:

  - Organisation of data;

  - Data model and data dictionary;

  - Encryption methods;

  - Method of updating if any (additions, overwriting or flagging obsolete entries)

- The semantic content of the data:

  - Coding schemes and identifiers used for particular data items;

  - Character sets and language of text.

If the Healthcards issued by Healthcard System-A and Healthcard System-B are identical in all these properties these Healthcard Systems are, by definition, technically interoperable. In this case the other components of the Healthcard access systems can either be identical may differ. If they can read and update Healthcards issued by their own system they must be technically capable of reading and updating Healthcards issued by the other system. However, it is possible for technical interoperability to include security provisions that deliberately prevent or restrict actual interoperability (see Section 5.6).

Limited interoperability may be achieved if the Healthcard issued by Healthcard System-A contains two or more different media and if one of these media is identical in all respects to one of the media used on a Healthcards issued by Healthcard System-B. Usually interoperability of this type will be symmetrical though it will be limited to functions supported by the data stored on the shared medium (see 5.3.2 and 5.3.3).

Otherwise interoperability will depend upon other Healthcard System components (see 5.5.2 and 5.5.3).

5.5.2 The Card Terminal

If the size, physical media and physical data formats of Healthcards issued by Healthcard System-A and Healthcard System-B are identical the same Card Terminal will usually be usable for Healthcards issued by either Healthcard System, even if the logical structure and semantics of the data differs. Interoperability then depends upon the ability of the interface-software to deal with different data structures (see 5.5.3).

Some Card Terminals contain programmable elements or are built into devices with input and/or output devices (e.g. keypads, built in screens, printers and slots for a health professional card containing keys to authorise access to the Healthcard). In these cases part of the interface is in effect built into the Card Terminal. Therefore, if either Healthcard System-A or Healthcard System-B uses such a Card Terminal, the Card Terminals of both Healthcard Systems must be able to carry out the functions of both. In these cases interoperability may be asymmetrical. A Card Terminal with additional built-in facilities may be able to process Healthcards that do not require these features but Healthcards that require the Card Terminal cannot be accessed by simpler Card Terminals. Conversely a Card Terminal that is built into a printer or other dedicated device may be unable to process other Healthcards because the interface is programmed within the Card Terminal. Even if the Card Terminal is physically identical, two Healthcard Systems may require programmable elements (e.g. EPROM/EEPROM) within the reader to be programmed differently.

Card Terminals capable of accessing different types of card media can be used to overcome problems associated with the use of Healthcards based on different technologies. The most widely available combination Card Terminals are able to read magnetic stripes, smart cards and other integrated circuit cards. Other combinations are possible but are not widely available and combinations including optical card readers are likely to be much more expensive. Card Terminals capable of accessing more than one media type may be significantly more expensive than single technology Card Terminals. In some cases it may be cheaper to install two separate Card Terminals but this can add to the difficulties of physically connecting the Card Terminals to the computer system or terminal. Healthcard Systems that attain interoperability by using dual combination Card Terminals must take account of data format, logical structure and semantic content and these depend on the interface-software (see 5.5.3). Unless both Healthcard System-A and Healthcard System-B have dual or combination Card Terminals, interoperability will be asymmetric (see 5.3.4). Unless all CASs in a Healthcard System have dual or combination Card Terminals interoperability will be location dependent (see 5.3.6).

5.5.3 Interface-software

If data on Healthcards issued by Healthcard System-A and Healthcard System-B share the same physical format, logical structure and semantics, then the interface-software will be interoperable. Provided that the Card Terminal and Healthcards are interoperable this may allow full symmetrical interoperability between Healthcard System-A and Healthcard System-B. However, the range of functions supported by the interfaces may be different and in this case interoperability may be asymmetric (see 5.3.4). For example, the interface provided to Healthcard System-B users may not be able to update cards. Similarly this type of discrepancy may result in location dependent limitations on interoperability (see 5.3.6). It is possible for technical interoperability to include security provisions that deliberately prevent or restrict actual interoperability (see Section 5.6).

If the physical format and logical data structure of Healthcards issued by one Healthcard System is a subset of the data-content of Healthcards issued by the other Healthcard System, interoperability may be possible using the same interfaces. This assumes that the data structures and interfaces of one Healthcard System allow:

- Additional data, present on Healthcards issued by other Healthcard Systems, to be ignored (rather than generating an error); and

- A limited range of functions to be performed on Healthcards that do not contain all the data items on Healthcards issued by that Healthcard System.

If the semantic content varies in terms of identifiers and coding schemes and character sets, an interface may be able to translate these if suitable cross-reference tables exist.

Interface-software can be developed that can recognise and process the data from different Healthcards. Alternatively, separate interface-software may coexist on the same CAS and may be selected automatically or manually according to the card type presented. As with combination Card Terminals the interoperability that results is likely to be asymmetric and location dependent (see 5.3.4 and 5.3.6).

As identified in section 6.5.5, one of the most flexible approaches to integration between a Healthcard System and a variety of different software applications is an openly specified Application Program Interface (API) for Healthcard access. A stable API allows the Healthcard and application software to develop independently while retaining compatibility. A common API shared by several Healthcard Systems also facilitates the development of interoperability between those systems.

5.5.4 User access, application software and databases

Figure 2 to Figure 5 illustrate different ways in which CASs can be structured. Information from the Healthcard can be communicated to the user either via an integrated application-database or directly from specialised software designed around the Healthcard data-set. There are similar variations in the options for an interoperable system (see Figure 15 and Figure 16).

- If a CAS participating in Healthcard System-A can access Healthcards issued by Healthcard System-B using the same interface-software used to access Healthcards issued by Healthcard System-A, then user access will follow the same approach whichever Healthcard System issued the Healthcard.

- If a CAS in Healthcard System-A uses different interface-software to access Healthcards issued by Healthcard System-B and does not support integration with a database, then user access will probably follow an approach that is specific to the issuing Healthcard System.

- If a CAS in Healthcard System-A uses different interface-software to access Healthcards issued by Healthcard System-B and supports integration of Healthcards from Healthcard System-A with an application database, then user access may be:

  - Directly through a user interface specific Healthcard System-B;
  - Via an integrated application and database specific to Healthcard System-B; or, preferably,
  - Via the same integrated application and database used by Healthcard System-A.

5.6 Security and enforcing interoperability agreements

Considerable care must be taken to ensure that access to Healthcards is restricted in a way that allows compliance with Interoperability .

When systems are made interoperable their security procedures must be reviewed. This is necessary to ensure that interoperability agreements between those responsible for the systems cannot be circumvented, either accidentally or maliciously (see Section 4). It is also important to be aware that interoperability risks creating loopholes which breach existing agreements with patients and users participating in existing systems.

5.6.1 The technical level at which security provisions are enforced

In a relatively small local Healthcard System, security provisions may be enforced within the interface or even within the application software. This may be acceptable where there are a small number of people responsible for the software development. Those involved can be legally bound, and then entrusted with knowledge that might allow them to breach the security provisions. For larger Healthcard Systems and certainly for interoperable systems there are more serious implications. The specification of the application-interface must be readily available to the developers of any application that needs to access a Healthcard. This poses a risk unless the security provisions are dealt with "below" the published interface (i.e. in the Card Terminal and/or the Healthcard itself). Ideally a password, authorisation card and PIN code or some form of biometric recognition mechanism should be accepted by the Card Terminal and used to authorise access to Healthcards. It may be acceptable for the PIN code and authorisation card data to be passed through the application and software interface but this poses a risk (as demonstrated by recent fraud cases in the US involving use of customised automatic teller machines to copy cash cards and PIN numbers).

Interoperability requires that the security mechanism can be specified in sufficient detail to allow it to be utilised by application developers involved in two or more Healthcard Systems without allowing them to unravel it.

5.6.2 Selectivity of access

If two Healthcard Systems that are to be made interoperable both enforce some form of selective access to different data items according to the user then interoperability introduces two complications:

- The data-items to which access is allowed by the same category of user may vary,
  - For example, in some Healthcard Systems entitlement to a healthcare service may be given a different security level from the medical record number while in others both may be treated as having similar sensitivity;
- The categories of users may vary,
  - For example, in some Healthcard Systems a dentist may be in the same health professional category as a doctor while in other countries they are in a separate category (possibly the same category as a pharmacist or a nurse).

5.6.3 Mobility of patients and professionals

A practical problem is posed by patients moving between the two Healthcard Systems. This is illustrated by the following scenario:

- A user of Healthcard System-A adds to a Healthcard a data-item which, in that Healthcard System, is only accessible to a doctor.

- The Healthcard is presented to a user of Healthcard System-B, in which the same data can be read by a receptionist.

- If the Healthcard Systems are interoperable, it may be difficult to enforce the correct access rights when the card is read and/or updated by either system.

Another problem is posed by staff moving between the two Healthcard Systems. This is illustrated by the following scenario:

- A dentist holds a Healthcare Professional Card issued by a Healthcard System-A, in which dentists and doctors have the same access rights.

- The dentist also works in an organisation using Healthcard System-B, in which dentists have a different level of authorisation.

- If their Healthcare Professional Card is interoperable, it may be difficult to enforce the distinctions between professionals in accord with the rules of both Healthcard Systems.

These problems are accentuated when the interoperable systems are in Member States with different data protection legislation.

A similar problem is caused by data items which may be recorded in some Healthcard Systems but may be contrary to data protection legislation in another Member States with an interoperable system.

These problems can be partially addressed by technical solutions but a longer term, more comprehensive solution requires harmonisation of the provisions for selective access.

5.6.4 Control of card issue

Healthcards may be used to confirm the identity and entitlement of patients to care. If this function is to be interoperable then those responsible for providing this entitlement will naturally be concerned to prevent fraudulent use of Healthcards. The manufacture, personalisation and distribution of Healthcard and the generation and distribution of PIN codes or other keys must be secure. If Healthcard Systems are interoperable a breach of security in one Healthcard System could damage the interests of those involved in the other Healthcard System.

5.6.5 Deliberately preventing interoperability

Even if identical Healthcards, Card Terminals, software and hardware are used in two separately managed Healthcard Systems, the Healthcard System management organisations may not agree to allow their systems to be interoperable. This may be because access to some or all of the Healthcard in the other scheme is unnecessary or because it increases the risks of error or fraud. Functional interoperability may therefore be blocked deliberately by use of different security codes or encryption keys. If these are distributed to users on data cards (e.g. health professional cards such as the French Carte Professional Santé) it may be possible to make systems interoperable after a subsequent agreement by simply distributing appropriate keys to users of the other Healthcard System.